日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 １月１９日

出願番号
Application Number: 特願２００１－０１１２５４

出願人
Applicant(s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年１１月３０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３１０５３０８

【書類名】　特許願

【整理番号】　2037330002

【提出日】　平成13年 1月19日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/32

H04L 9/30

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　水山　正重

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　小林　卓也

【発明者】

【住所又は居所】　神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内

【氏名】　加藤　淳展

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　コンテンツ署名検証方式

【特許請求の範囲】

【請求項１】署名者が電子署名可能なコンテンツ種別を、前記署名者に対して発行する署名者証明書に記載しておき、電子署名されたコンテンツを受信したエンティティが前記電子署名を検証する際に、前記署名者証明書に記載された前記コンテンツ種別と受信した前記コンテンツのコンテンツ種別が一致した場合にのみ署名を有効とすることを特徴とするコンテンツ署名検証方式。

【請求項２】署名者が電子署名可能なコンテンツ種別を、リスト形式で複数記載できることを特徴とする請求項１記載のコンテンツ署名検証方式。

【請求項３】署名者が電子署名可能なコンテンツ種別としてワイルドカードを指定すると全てのコンテンツ種別に対して署名可能となることを特徴とする請求項１記載のコンテンツ署名検証方式。

【請求項４】コンテンツ種別をコンテンツのURIの拡張子部分によって指定することを特徴とする請求項１記載のコンテンツ署名検証方式。

【請求項５】コンテンツ種別をコンテンツ受信時のヘッダ情報に含まれるコンテンツ種別情報によって指定することを特徴とする請求項１記載のコンテンツ署名検証方式。

【請求項６】前記署名者証明書は、コンテンツに対する電子署名と共に送信されることを特徴とする請求項１記載のコンテンツ署名検証方式

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子署名の署名者に限定的署名権限を付与する手段に関するものである。

【０００２】

【従来の技術】

従来、電子署名によるコンテンツの安全性、妥当性を検証する場合、署名者がどのようなコンテンツに対して署名できるかという情報に関しては、応用システ

ムの中で個別に暗黙に決定されていたり、認証局が証明書に付与する証明書の「クラス」や証明書の「用途」によって大まかに区分された属性情報に基づいて、アプリケーションによって解釈をその都度定めて判定を行うという方式が取られてきた。

【０００３】

【発明が解決しようとする課題】

しかしながら、近年XMLを用いた電子商取引への応用など、セキュリティを確保する必要のあるコンテンツの爆発的多様化の兆しが見えており、コンテンツの種別が多様化しても署名者の権限を、コンテンツの種別に依存せず同一の方法で判定できることが必要となっている。コンテンツの目的やそのコンテンツを受け取ったときに受信システムが行うべき処理の内容は、コンテンツの種別と対応関係にある場合が多くある。従来の技術では、このような場合に署名者の署名権限を定める共通的な規則が存在しないため、コンテンツの種別が増えた場合に、新しいコンテンツの種別に関してどのような署名者が署名権限を付与されていると判定するかに関しては、新しいコンテンツが増える都度、応用システムとして個別の判定論理を実装しなければならないという問題があった。

【０００４】

【課題を解決するための手段】

この課題を解決するために本発明は、署名者証明書の中に、その署名者が署名可能なコンテンツ種別を明記し、署名検証を行うエンティティがコンテンツの種別と署名者証明書を取得できれば、コンテンツの種別によらず同一の方法でその署名者がそのコンテンツに署名する権限をもっているかどうかを判定する手段を提供するものである。

【０００５】

本発明の請求項1に記載の発明は、署名者が電子署名可能なコンテンツ種別を、前記署名者に対して発行する署名者証明書に記載しておき、電子署名されたコンテンツを受信したエンティティが前記コンテンツの電子署名を検証する際に、前記コンテンツの署名者に発行された署名者証明書に記載された前記コンテンツ種別と受信した前記コンテンツのコンテンツ種別が一致した場合にのみ署名を有

効とするものであり、これによって、任意の種別のコンテンツに関しても、同じアルゴリズムで、署名者が当該コンテンツに対して署名権限を持っているかどうかを判定することができるという作用を有する。

【０００６】

本発明の請求項２に記載の発明は、請求項１に記載の発明において、署名者が署名可能なコンテンツ種別を、リスト形式で複数記載できるようにするものであり、これによって、署名者が複数のコンテンツ種別に対して署名権限を持っていることを単一の署名者証明書で表現できるという作用を有する。

【０００７】

本発明の請求項３に記載の発明は、請求項１に記載の発明において、署名者が署名可能なコンテンツ種別としてワイルドカードを指定すると全てのコンテンツ種別に対して署名可能であると見なすものであり、これによって、署名者が全てのコンテンツ種別に対して署名権限を持っていることを、証明書に全てのコンテンツ種別を列挙することなく表現できるという作用を有する。

【０００８】

本発明の請求項４に記載の発明は、請求項１に記載の発明において、コンテンツ種別をコンテンツのURIの拡張子部分によって指定するものであり、これによって、署名を検証するエンティティは、コンテンツのURIの拡張子部分と、署名者証明書に含まれる署名可能なコンテンツ種別の情報を文字列として比較することで、署名者が当該コンテンツに署名する権限を持っているか否かを判定することができるという作用を有する。

【０００９】

本発明の請求項５に記載の発明は、請求項１に記載の発明において、コンテンツ種別をコンテンツ受信時のヘッダ情報に含まれるコンテンツ種別情報によって指定するものであり、これによって、署名を検証するエンティティは、コンテンツの受信時のヘッダ情報に含まれるコンテンツ識別情報と、署名者証明書に含まれる署名可能なコンテンツ種別の情報を文字列として比較することで、署名者が当該コンテンツに署名する権限を持っているか否かを判定することができるという作用を有する。

【００１０】

本発明の請求項６に記載の発明は、前記署名者証明書が、コンテンツに対する電子署名と共に送信されることを特徴とするものであり、これによって、受信者が予め当該コンテンツに対する署名者の署名者証明書を所有していない場合にでも、署名者の権限を判定可能になるという作用を有する。

【００１１】

【発明の実施の形態】

次に本発明の実施例を図面と共に説明する。図1は本発明が適用されるシステムの一実施例の構成を示すブロック図であって、１１はコンテンツサーバ、１２はネットワーク、１３はコンテンツ処理装置である。図２は本発明の適用されるコンテンツの一実施例であって、以下の説明で参照するために各行に行番号を割り振っている。図３は本発明の適用される署名者証明書の一実施例であって、同じく以下の説明で参照するために各行に行番号を割り振っている。図２のコンテンツおよび図３の署名者証明書は、共にXMLと同様に「＜タグ＞情報＜／タグ＞」の形式で、タグとそれに対応する情報を記述する。タグに対応する情報自体が「＜タグ＞情報＜／タグ＞」の形式をとるような階層構成が可能である。

【００１２】

コンテンツサーバ１１とコンテンツ処理装置１３は、ネットワーク１２を介して接続されているものとする。コンテンツサーバ１１に図２に示すような形式のコンテンツが格納され、コンテンツ処理装置１３からネットワーク１２経由で到着するコンテンツ取得要求に応じてコンテンツ処理装置１３に送出される。コンテンツ処理装置１３は図２に示すような形式のコンテンツを受信すると、コンテンツに対応する処理を行う前に、次のような手順で受信したコンテンツを検証する。

【００１３】

コンテンツ処理装置１３は、行番号（２０２）のｓｉｇｎｅｄＢｙタグに対応する署名者の名前（図２のコンテンツ例では「ＸＹＺ株式会社」）に対応する署名者証明書を、内蔵する署名者証明書データベース１４から取得する。これは、署名者証明書のＳｕｂｊｅｃｔタグの値が、当該コンテンツのｓｉｇｎｅｄＢｙ

タグの値に一致するものを署名者証明書データベース１４中から検索することによって得られる。こうして得られた署名者証明書が図３に示す証明書であるとする。コンテンツ処理装置１３は、署名者証明書の行番号（３０５）に書かれたＡｕｔｈｏｒｉｚｅｄＣｏｎｔｅｎｔＴｙｐｅｓタグの値に、今回受信したコンテンツの種別に該当するものが含まれているかどうかをチェックする。ＡｕｔｈｏｒｉｚｅｄＣｏｎｔｅｎｔＴｙｐｅｓタグの値に含まれているのはａｄｒｓとｓｃｈｅｄというコンテンツ種別である。コンテンツの種別が、コンテンツのＵＲＩの拡張子によって決定されるような応用例では、受信コンテンツのＵＲＩの拡張子がａｄｒｓかｓｃｈｅｄのいずれかである場合に、コンテンツ処理装置１３は、前記署名者が、前記コンテンツに署名する資格があると判定する。今回受信したコンテンツのＵＲＩの拡張子がａｄｒｓであったとすると、コンテンツ処理装置１３は、前記署名者が前記コンテンツに署名する資格があると判定して、署名者証明書の行番号（３０６）のＰｕｂｌｉｃＫｅｙタグの値として設定されている公開鍵を使用して、図２のコンテンツの行番号（２１０）のｓｉｇｎａｔｕｒｅタグの値として設定されている電子署名を検証する。具体的には、図２のコンテンツの行番号（２０１）、（２０９）のｓｉｇｎｅｄＩｎｆｏタグの値である行番号（２０２）～（２０８）の文字列に対してＭＤ５などのハッシュ関数を適用して計算したハッシュ値と、行番号（２１０）のｓｉｇｎａｔｕｒｅタグの値である電子署名値を前記公開鍵で復号化した値を比較し、一致していた場合に電子署名が正しいと見なす。そうでない場合には電子署名が異常であると見なして当該コンテンツを破棄する。

【００１４】

上記実施例では、コンテンツの種別がコンテンツのＵＲＩの拡張子によって指定されるものとして説明したが、コンテンツ受信時のヘッダ情報に含まれるコンテンツ種別情報によって指定されるような実施例も考えられる。

【００１５】

また、署名者証明書のＡｕｔｈｏｒｉｚｅｄＣｏｎｔｅｎｔＴｙｐｅｓタグの値として＊（アスタリスク）が指定されていた場合には、コンテンツ処理装置１３はいかなるコンテンツ種別のコンテンツに対しても前記署名者証明書で指定さ

れる署名者は署名権限をもっていると判定するような実施例も考えられる。

【００１６】

更に、コンテンツ処理装置１３がコンテンツサーバ１１からコンテンツを受信時に、コンテンツと共に署名者証明書がコンテンツサーバ１１から受信されるような実施例も考えられる。この場合には署名者証明書データベース１４に含まれない署名者に関しても、署名者の権限チェックが可能になる。このような場合、虚偽の署名者証明書がコンテンツサーバ１１から送信された場合にコンテンツ処理装置１３がそれを検出できるように、署名者証明書に認証局の署名をしておくといった実施形態が考えられる。

【００１７】

【発明の効果】

以上詳細に説明したように、本発明によれば、署名者の署名権限を、署名可能なコンテンツ種別という形で署名者証明書中で定義できるために、新たなアプリケーションの出現に対応して新しい種別のコンテンツを扱う必要が出てきた場合でも、権限判定方式を変更することなく適用することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態のシステムの一実施例の構成を示すブロック図

【図２】

本発明の実施の形態のコンテンツのフォーマットの一例を示す図

【図３】

本発明の実施の形態の署名者証明書のフォーマットの一例を示す図

【符号の説明】

１１　コンテンツサーバ

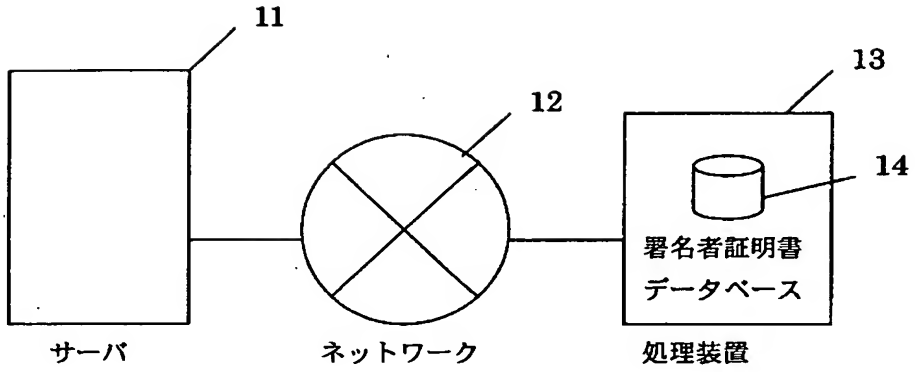
１２　ネットワーク

１３　コンテンツ処理装置

１４　署名者証明書データベース

【書類名】　　図面

【図１】



【図２】

```
(行番号)
(201) <signedInfo>
(202) <signedBy>XYZ 株式会社</signedBy>
(203) <command>AddToAddressBook</command>
(204) <parameters>
(205) <name>ABC 商事</name>
(206) <fax>06-1234-5679</fax>
(207) <phone>06-1234-5678</phone>
(208) </parameters>
(209) </signedInfo>
(210) <signature>sZsiuHJmx40HwJ6JZzxkiwsq2</signature>
```

【図３】

```
(行番号)
(301) <Subject>XYZ 株式会社</Subject>
(302) <Issuer>JJJ 認証局</Issuer>
(303) <NotBefore>2000/01/01</NotBefore>
(304) <NotAfter>2010/12/31</NotAfter>
(305) <AuthorizedContentTypes>adrs,sched</AuthorizedCont
      entTypes>
(306) <PublicKey>Ajsi8Jas0Ihswwcuy82xIsJelM</PublicKey>
(307) <Signature>sNJAUhgsw8J9Jhheasi9xjiads</Signature>
```

【書類名】　要約書

【要約】

【課題】　電子署名によってコンテンツの安全性や妥当性を検証する場合において、署名者がどのようなコンテンツに対して署名できるかについての判定する場合、新しいコンテンツ種別が増えても、権限判定方式を変更することなく対応可能な判定手段を提供する。

【解決手段】　署名者証明書の中に、署名者が署名可能なコンテンツ種別を記述することで、署名検証を行うエンティティがコンテンツの種別と署名者証明書を取得した場合に、署名者がそのコンテンツに署名をする権限を持っているかどうかの判定を可能とする。

【選択図】　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社